

Response Under 37 C.F.R. §1.111  
Serial No. 10/069,118  
Attorney Docket No. 020234

### **REMARKS**

Claims 23-63 are pending in the above-identified application. It is respectfully submitted that this response is fully responsive to the Office Action dated April 28, 2006.

#### **Non-Responsive To Applicants' Previous Remarks**

An examiner is required to provide clear explanations for all actions taken by the examiner during prosecution of an application." MPEP 707.07(f) (The examiner should "take note of the applicant's argument and answer the substance of it.") This requirement is in addition to any repetition of a previously held position and is required to allow the Applicant a chance to review the Examiner's position as to these arguments and to clarify the record for appeal. However, in this Action, the Examiner failed to address the substance of Applicants' remarks provided in the June 16, 2005 and the March 2, 2006 Amendments. Thus, the Applicants have not had the chance to review the Examiner's position to determine whether to further clarify the record for possible appeal. Accordingly, Applicants respectfully request that the Examiner withdraw the objections to claims 23-63.

However, in an effort to expedite prosecution and clarify the present invention, Applicants hereby address the following three-points presented by the Examiner:

(1) *How the first description key is generated and obtained.*

Applicants respectfully submit that the "first decryption key" recited in claims 23 and the like corresponds to private decryption key Kp that is paired with public encryption key Kpp. This "first decryption key", for example, is a preset key unique to the cellular phone corresponding to the data

reproduction apparatus for data communication using public encryption key techniques. In other words, this key is provided from the beginning and is not a generated key.

*(2) If the content key is encrypted with the first key, how the session key is able to decrypt the encrypted content.*

Applicants first describe an example of the flow of the process in the present invention. In this example, the "data reproduction apparatus" recited in claim 23 corresponds to cellular phone 200, "data reproduction unit" corresponds to audio reproduction module 1500, and "data storage unit" corresponds to memory card 120.

Encrypted content data [Dc] Kc and encrypted content key [Kc] Kp are stored in memory card 120. Encrypted content data [Dc] Kc is an encrypted version of content data Dc with content key Kc. Encrypted content key [Kc] Kp is an encrypted version of content key Kc with public encryption key Kp unique to audio reproduction module 1500. Encrypted content key [Kc] Kp encrypted with public encryption key Kp can be decrypted using private decryption key Kp unique to audio reproduction module 1500.

Audio reproduction module 1500 generates, at Ks generator 1502, a session key Ks that is updated at every access to obtain a content key Kc with respect to memory card 120. Audio reproduction module 1500 encrypts the generated session key Ks with public encryption key Kpm that is unique to memory card 120 and outputs the encrypted key to memory card 120.

Memory card 120 uses private decryption key Km unique to memory card 120 to decrypt the session key that has been encrypted with public encryption key Kpm output from audio reproduction module 1500.

Accordingly, memory card 120 obtains session key  $K_s$ .

Memory card 120 further encrypts encrypted content key  $[K_c] K_p$  using the obtained session key  $K_s$ , and outputs the further encrypted encryption content key  $[[K_c] K_p] K_s$  to audio reproduction module 1500.

Audio reproduction module 1500 uses session key  $K_s$  generated at  $K_s$  generator 1502 to decrypt the further encrypted encryption content key  $[[K_c] K_p] K_s$  to obtain encrypted content key  $[K_c] K_p$ .

Audio reproduction module 1500 decrypts encrypted content key  $[K_c] K_p$  using private decryption key  $K_p$  unique to the audio reproduction module to obtain content key  $K_c$ .

Audio reproduction module 1500 uses content key  $K_c$  to decrypt encrypted content data  $[D_c] K_c$  to obtain content data  $D_c$ .

The invention of the present application, for example, is based on a system, not simply outputting encrypted content data  $[D_c] K_c$  and encrypted content key  $[K_c] K_p$  to audio encryption module 1500 from memory card 120, but transferring and receiving a session key  $K_s$  that is updated at every access, and encrypting again encrypted content key  $[K_c] K_p$  using session key  $K_s$ , and then outputting encrypted content data  $[D_c] K_c$  and encrypted content key  $[K_c] K_p$  from memory card 120 to audio reproduction module 1500.

The present system is advantageous, for example, because the encrypted content key  $[K_c] K_p$  cannot be viewed directly from an external source by virtue of re-encryption using session key  $K_s$ . Thus, security is improved because it is difficult to illegally obtain the encryption scheme and private decryption key of cellular phone 200 from an external source.

Thus, the Examiner's point ("if the content key is encrypted with the first key, how is the session key able to decrypt the encrypted content?") can be appreciated from the fact that an encryption process is applied twice to the content key, as described in the example above.

Furthermore, to summarize, encrypted content key [Kc] Kp stored in memory card 120 is an encrypted version of content key Kc with public encryption key KPp unique to audio reproduction module 1500.

Encryption content key [[Kc] Kp] Ks output from memory card 120 to audio reproduction module 1500 is a further encryption of encrypted content key [[Kc] Kp] with session key Ks.

By this double encryption process set forth above, the further encrypted encryption content key [[Kc] Kp] Ks output from memory card 120 to audio reproduction module 1500 is decrypted into encrypted content key [Kc] Kp by session key Ks.

Then, the encrypted content key [Kc] Kp that is encrypted with public encryption key KPp (first key) is decrypted into content key Kc by private decryption key Kp unique to audio reproduction module 1500.

*(3) Why there is a need for a second decryption processing unit to extract the content key if the encrypted content key was already decrypted at a first decryption processing unit.*

Applicants respectfully submit for example, that the encrypted content key [Kc] Kp stored in memory card 120 is an encrypted version of content key Kc with public encryption key KPp unique to audio reproduction module 1500, and encryption content key [[Kc] Kp] Ks output from memory card 120 to audio reproduction module 1500 is a further encrypted version of encrypted content key [Kc] Kp with session key Ks.

Therefore, decryption processing unit 1506 uses session key  $K_s$  to decrypt encryption content key  $[[K_c] K_p]$   $K_s$  output from memory card 120 to audio reproduction module 1500 into encrypted content key  $[K_c] K_p$ . Then, decryption processing unit 1530 uses private decryption key  $K_p$  unique to audio reproduction module 1500 to decrypt encrypted content key  $[K_c] K_p$  into content key  $K_c$ .

Thus, because content key  $K_c$  is subjected to a double encryption process, a double decryption process is also required, *i.e.* one decryption at each of the two decryption processing units.

#### **Claim Objections - §112**

Claims 23, 28, 34, 45 and 53 were objected to because it is unclear to the Examiner “which portion of these claims is preamble and which portion is body of the claim.” Applicants disagree with the Examiner’s position. Where the preambles end and the body of the claims start is clear from wording in the claims (*e.g.*, transitional words.) Accordingly, Applicants respectfully request that the Examiner withdraw the objection to these claims.

Claims 23-63 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Specifically, claims 23, 28, 34, 45 and 53, were rejected because, according to the Examiner, it is unclear what the difference between the content key, decryption key, encryption key, session key and public key is. The Examiner asserted that the terms are being used interchangeably which makes it difficult to identify the scope of the claims. Applicants respectfully disagree with the Examiner’s position because, interpreted properly, it is clear that the terms are not being used interchangeably in the claims. Furthermore, the Examiner misinterpreted these claims as including an encryption key

Response Under 37 C.F.R. §1.111  
Serial No. 10/069,118  
Attorney Docket No. 020234

and a public key (only a “public encryption key” is described in the above claims.) Accordingly, Applicants respectfully request that the Examiner withdraw this rejection.

The Examiner also stated that is unclear what the first and the second encryption units do in regards to encrypting the keys and the content as far as the claims go. However, these claim features are clearly defined, for example, on page 3, lines 10-13 of the specification and in the claims. Accordingly, Applicants respectfully request that the Examiner either withdraw this reason for rejection or indicate *why* these claim elements are indefinite.

In addition, the Examiner stated that the difference between the first session key and the second session key is unclear. However, Applicants respectfully submit that these claim elements are clearly explained, for example, on page 3, lines 8-13 and page 3-1, lines 6-22 of the specification and in the claims. Accordingly, Applicants respectfully request that the Examiner either withdraw this reason for rejection or indicate *why* these claim elements are indefinite.

Claims 26, 49 and 57 were also rejected because it is unclear to the Examiner which key is used to encrypt the session key and where the session key is being encrypted (because the claims recite using the private key to encrypt the session key and then the claim recites using the public key to encrypt the session key.) Claims 31, 37 and 43 were rejected because it is unclear to the Examiner which session key is used to obtain the content key or the decryption key. Claims 33, 35, 44, 46 and 54 were rejected because it is unclear to the Examiner what is meant by authentication key or if the authentication key is being used interchangeably with public private key. Claims 37 and 43 were also rejected because it is not clear to the Examiner what is the difference between the unique decryption key in claim 12 and the second decryption key in claims 15 and 21.

Response Under 37 C.F.R. §1.111  
Serial No. 10/069,118  
Attorney Docket No. 020234

Applicants respectfully disagree with the Examiner's position on these claim rejections. The Examiner has failed to point out *why* these claim elements are indefinite. Also, the specification and claims properly explain the above claim elements.

**Claim Rejection - §102(e)**

Claims 23-63 were rejected under 35 U.S.C. 102(e) as being anticipated by *Ginter et al.* (U.S. Pat. No. 5,917,912). However, anticipation requires the presence in a single prior art reference the disclosure of each and every element of the claimed invention, arranged as in the claim. As discussed below, *Ginter et al.* fails to disclose several elements of the claimed invention. Accordingly, Applicants respectfully submit that *Ginter et al.* is not a proper §102 reference. Thus, in view of the following remarks, Applicants respectfully request that the Examiner withdraw the anticipation rejection of claims 23-63.

In rejecting these claims, the Examiner asserted that the reference discloses “a session key generation unit generating a session key updated at every access to obtain said content key with respect to said data storage unit”; and “a first encryption processing unit encrypting said session key using a public encryption key that can be decrypted at said data storage unit and that is unique to said data storage unit, and providing said encrypted session key to said data storage unit”.

However, *Ginter et al.* does not disclose the features recited in claims 23, 28, 34, 45, and 53. For example, *Ginter et al.* teaches that “(Party) A must create the (session) key, prove that A created it, and prove that it is associated with the specific proposed communication...(and) the session key must be protected from disclosure of modification to ensure that an attacker cannot substitute a

Response Under 37 C.F.R. §1.111  
Serial No. 10/069,118  
Attorney Docket No. 020234

different value.” [col. 219, lines 31-39.] *Ginter et al.* does not teach or disclose that the session key is encrypted. Encrypting said session key makes it is difficult for a third party (unauthorized user) to improperly access distribution data as to content data stored in a memory by a proper user. *See*, for example, page 3/4, lines 8-12.

Moreover, *Ginter et al.* does not teach or disclose that the session key is updated at every access to obtain a content key with respect to the data storage unit and that a first encryption processing unit encrypts the session key using a public encryption key that is decryptable at the data storage unit and unique to the data storage unit, and provides the encrypted key to the data storage unit. The first decryption processing unit uses the session key to decrypt the encrypted content key obtained from the data storage unit in a form encrypted by the session key. *See*, for example, page 3, lines 8-13.

Accordingly, Applicants respectfully request that the Examiner withdraw the §102(e) rejection of claims 23, 28, 34, 45 and 53.

Moreover, as claims 24-27, 29-33, 35-44, 46-52, and 54-63 depend from independent claims 23, 28, 34, 45 and 53, respectively, these claims should likewise be allowable in view of the above comments by nature of their dependency.

For at least the foregoing reasons, the claimed invention distinguishes over the cited art and defines patentable subject matter. Favorable reconsideration is earnestly solicited.


Should the Examiner deem that any further action by applicants would be desirable to place the application in condition for allowance, the Examiner is encouraged to telephone applicants' undersigned attorney.

Response Under 37 C.F.R. §1.111  
Serial No. 10/069,118  
Attorney Docket No. 020234

If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

**WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP**

A handwritten signature in black ink, appearing to read "Darrin A. Auito", is written over a circular stamp or seal.

Darrin A. Auito  
Attorney for Applicants  
Registration No. 56,024  
Telephone: (202) 822-1100  
Facsimile: (202) 822-1111

DAA/rf/mra